Mississippi Department of Information Technology Services

FOR YOUR INFORMATION

January/March 2011

INSIDE THIS ISSUE

Mississippi E-Government

By Renee' Murray
Department of Information Technology Services

In 2000, ITS in conjunction with the Department of Finance and Administration (DFA) and on behalf of participating Mississippi E-Government Task Force agencies, issued RFP 3205 to establish an E-Government framework for the State of Mississippi. The goals and objectives of RFP 3205 were to provide for electronic payments to state agencies, launch on-line services by providing 4 pilot applications, and deploy a redesigned State website.

The infrastructure put in place as a result of RFP 3205 has supported over 200,000 transactions each of the last 2 fiscal years, generating over 1.3 million dollars in revenue that has been used to support and further develop the E-Government infrastructure. At the end of the initial contract, application development and support activities transitioned to the state and many new applications have been deployed. The redesigned MS.gov has become the portal or entry way to State Government and averaged about 6,000 visits per day during the last fiscal year.

MS.gov has had only one minor redesign since its launch in 2001. The initial contract with the State's payment services vendor has reached end-of-life and must be replaced. Seeing this as an opportunity to expand E-Government in the state, ITS and DFA issued RFP 3564 seeking a vendor partnership to enhance E-Government offerings and provide for a new payment services vendor.

At the ITS board meeting in December 2010, a contract was awarded to a local company, Mississippi Interactive, which is a subsidiary of NICUSA. NICUSA currently has partnership arrangements with 23 other states and supports E-Government services for 3,500 agencies and divisions of state, federal and local government. Provisioning of E-Government and payment services is their sole line of business and they offer a robust inventory of developed applications.

Through this partnership, Mississippi Interactive, ITS, and DFA have several high level objectives including: an updated MS.gov website; an increased number of E-Government applications, developed and deployed quickly and inexpensively; increased options for payment services including kiosks and Point-of-Sale (POS) devices; the use of mobile applications; incorporation of social networking into state applications and websites; and, enhanced web content management options for use by state agencies.

The business model proposed by Mississippi Interactive is a self-funded model whereby many applications and services can be provided at no

Mississippi E-Government

Continued from page one

direct cost to the state. No initial investment by the state is required and the program will be supported through fees associated with commercial access to state data rather than through fees assessed to citizen transactions or related to citizen access to data.

Work is already underway to establish the integration of the new payment service with existing state applications. Look for more information about how Mississippi continues to benefit from this new partnership in the months to come.

State Data Center Technology Updates

By Mitchell Bounds
Department of Information Technology Services

The new ITS Data Center facility is now functionally complete and ITS will be moving most of the processing capacity from the old downtown location to the new location. Expect a gradual migration of test and quality assurance platforms from the old center to the new center over the next few months. Tentatively, the mainframe environment will be moved around the first weekend in May, with much of the production open systems environments following over the next weeks.

The new Data Center will provide functionality exceeding that of the present Data Center. The new Data Center is:

- Hardened to provide protection against most natural and man-made disasters.
- Constructed to provide complete redundancy in all electrical and mechanical systems.
- More physically secure.
- Engineered so that everything in the physical plant can be monitored both remotely and on-site.
- Constructed to substantially increase the available Data Center floor space and allow for further expansion as necessary.

The ITS staff is preparing to move the Data Center with a minimum of downtime for existing and/or new applications. Some of the techniques used for the migration are:

- Extending the Data Center network and SAN environment over the state fiber to the new center so that servers have access to any resource in either center, facilitating a gradual migration.
- Locating new hardware platforms in the new center to minimize physical equipment moves.
- Employing VMware Vmotion and AIX Live Partitioning Mobility so that server instances can be moved “on the fly.”
- Using data movement software such as FDRPAS (move mainframe data) and metro-mirror software to move data over fiber so that data can be staged before physical moves of equipment occur.
- Locating equipment for pending, new applications and operating the equipment housing the new applications within the new center environment, minimizing the amount of equipment moves required.

To further enhance the availability and security of the data housed at new State Data Center, ITS now expects that the present Data Center will be

State Data Center Technology Updates

Continued from page two

retained, allowing the development of a more complete business recovery plan. The second Data Center will not only provide for state owned disaster recovery facilities but will also facilitate any cooperative processing such as replication and offsite backup.

z/OS Conversion

By Mitchell Bounds
Department of Information Technology Services

To ensure that the mainframe operating system runs on a supported release, the ITS Data Services staff will be converting the z/OS operating system from z/OS 1.9 to z/OS 1.11. At this time the conversion for CPU1 (the main production system) is scheduled for March 13. Conversion for CPU2 (MDHS production system) will be scheduled for the first week in May. All test systems have been operating on z/OS 1.11 for six months without problems.

The noticeable differences in the two versions are minimal for most users of the z/OS (mainframe) environment. However, there are many software product upgrades (such as to CA products) and many customization parameters that must be retained from z/OS release to z/OS release. On occasion, parameter defaults change or the systems staff misinterprets a new parameter and problems do occur. Testing will catch 99% of problems, but there are issues with each release when production applications systems are started on a new z/OS environment.

If any user of the mainframe environment would like to test an existing application on z/OS 1.11 before the conversion, please call the Helpdesk at 601-432-8080 and someone will contact you and set up a test environment.

Top Security Threats for 2011

By AliceClaire Thompson
Department of Information Technology Services

Technology change shows no signs of slowing. As it evolves, cyber criminals continue to educate themselves on the new processes and gadgets. With their progressing education comes a constant surge of brand new security threats to businesses as well as the basic home user. With the New Year enters yet another new crop of security threats. The following is a list of what we see to be some of the top security threats of 2011.

Social Media

It’s no surprise that one of the top security threats for 2011 is Social Media. According to Hitwise, a global online intelligence service which collects data directly from ISP networks, Facebook.com was the top visited website in the U.S. in 2010, making up 8.93% of site visits between January and November 2010. Google.com came in second at 7.19%. One of the main problems with social media use these days comes from users placing complete trust in online communities and inputting too much information, resulting in their sensitive data being exposed. When you combine over 500 million users, the false sense of trust that social media sites project, and hundreds of potential security issues, you have nothing less than a recipe for disaster. Social network users can expect to see

Top Security Threats for 2011

Continued from page three

a surge in viruses that spread throughout entire friend lists and online communities circulated by a simple click of mouse on a well-known link. Viruses already exist that capture banking and credit card information as well as other personal data you have entered into the site, which leads to an increase in identity theft. These sites are the perfect environments for criminals to slip malicious code into posts or messages on a site where users' attention to security is faint.

Mobile Devices/Smart phones

Many believe that just as 2010 was the year of the mobile device, 2011 will be the year of the mobile device security breach. While Apple has stricter procedures on accepting applications into their App Store for their devices, both Google and Apple have begun to see more vulnerabilities in each of their platforms. These mobile devices are widely used, but relatively insecure, which leaves workplace networks at risk. As employees become increasingly mobile and continue to use the same devices for both business and personal use, threats to network security will increase. The lines between business and personal use continue to blur and 2011 could easily be the year that mobile devices become the leading source of confidential data loss and identity theft. IT security specialists need not only look into securing employees mobile devices but also educating the users as now, more than ever, the responsibility for security lies almost solely in the hands of the user.

According to Patrick Traynor, assistant professor at Georgia Tech's School of Computer Science, "while more than 1.5 billion people use the Internet daily, over 4.5 billion use a cell phone every day, creating an attractive target for cyber criminals."

Malware-as-a-Service

Malware-as-a-Service is expected to become widespread in 2011. According to M86 Security Labs recent research, different players within the world of cybercrime are now offering their products as a service. Criminals are teaming up in hopes of creating a one-stop shop for cybercrime-as-a-service capabilities. Knowing the interworking of cybercrime is no longer needed because hiring a hacker is virtually a mouse click away. Now, as long as the right figures are available in your bank account, anyone can hire an expert cyber criminal to hack into a computer system and steal information or install malicious viruses on machines to crash entire networks.

Mac/Apple

Mac users have always felt virtually untouched by the spread of malware and other security threats. The thought has always been that while PCs might be vulnerable to such attacks, Mac operating systems were more resilient and unbreakable to even the sneakiest cyber attack. Now fast forward to 2011. Within the past three years over 100 million Apple products (iPad, iTouch, iPhone) have been sold and their popularity continues to increase. These products become more attractive to cybercriminals as their popularity grows. In 2010 we saw a boom in threats to Mac devices and there are no signs of this slowing down anytime soon. Malware for Mac does, indeed, exist and will continue to flourish as the market for its products continues to surge around the world. Crooks go where people are, and at this point the target is most definitely Apple.

Botnets

Botnets have always been a major concern in the cyber community because of their automation and large-scale capabilities. Botnets collectively generate 95% of the world's spam and have

Top Security Threats for 2011

Continued from page four

infected an estimated 100 million computers. Adrienne Hall, general manager for Microsoft Trustworthy Computing, suggests that most of today's computer criminal activity starts with botnets, "Botnets are the launch pad for much of today's criminal activity on the Internet. In many ways, they are the perfect base of operations for computer criminals." While more attention than ever is being paid to botnets, the attacks continue to multiply. Malware developers may be thwarted by small victories to shut botnets down, but the problem is that these developers simply create new bots and bot variants significantly faster than the attacks can be stopped. On all levels, however, security is getting more attention, which will hopefully ignite a proactive approach to the botnet security threat.

Social Engineering

Social Engineering will continue to be a prominent threat in 2011. It is suspected that there will be fewer malicious websites this year; instead, cyber criminals will put their energy into large malware campaigns. These campaigns will promote the threats via well-designed email messages that trick users into clicking infected links that in turn download viral files onto your machine. Cyber criminals will use Social Engineering attacks more frequently as a means to get around security controls instead of trying to break through them, simply by tricking people into turning over their own information.

Attacks via USB

We all have one, somewhere, whether it be hanging on a lanyard around your neck or tucked away in the back of a filing cabinet. USB drives are as frequent a giveaway as a Wal-Mart gift card. The threats associated with these thumb drives continue to increase as the devices become less expensive and data is increasingly distributed on them at trade shows and conferences across the country. Narus, a supplier of network security products, has named this as one of the top security threats for this year. Chief marketing officer David Friendman says that one out of every eight malware attacks on computers enters via a USB device. Unassuming users receive a freebie at a conference and think nothing of plugging the device into their machine to store data, not knowing that data with malicious intent has already been set up on the drive and programmed to run immediately once connected. Yet again, educating users is the most effective defense against this attack.

> *...educating users is the most effective defense against this attack.*

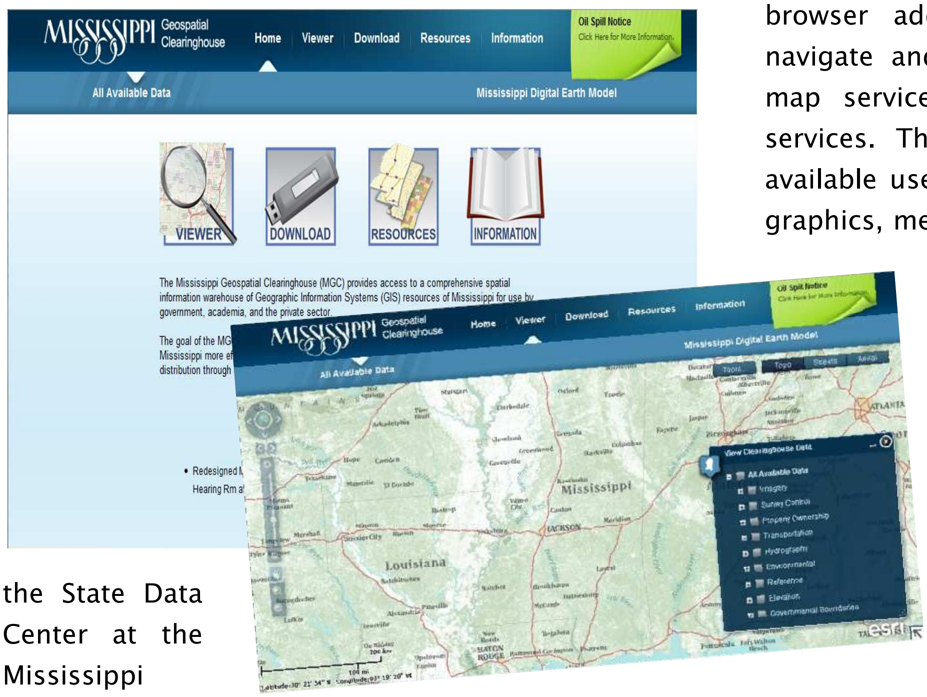
The Mississippi Geospatial Clearinghouse Upgrade

By Debra Brown
Department of Information Technology Services

The Mississippi Geospatial Clearinghouse (MGC) was placed in production in September 2007 and serves as the state's premier portal for the Geographic Information System (GIS) community to search, discover, share, and use a comprehensive warehouse of Mississippi's geospatial resources. The goal of the MGC is to make the application of spatial information GIS technologies within the state of Mississippi more efficient by eliminating the duplication of spatial data production and distribution through cooperation, standardization, communication, and coordination. Moreover, the MGC is the primary location for the Mississippi Digital Earth Model (MDEM). The MGC is housed in

The Mississippi Geospatial Clearinghouse Upgrade

Continued from page five



The Mississippi Geospatial Clearinghouse (MGC) provides access to a comprehensive spatial information warehouse of Geographic Information Systems (GIS) resources of Mississippi for use by government, academia, and the private sector.

The goal of the MG
Mississippi more ef
distribution through

• Redesigned
Hearing Rm a

the State Data Center at the Mississippi Department of Information Technology Services (ITS).

State agencies, county government, city government and the public can download data that has been stored in the MGC. This data provides the foundation for applications to be developed using GIS technology to meet business needs of the governmental agencies and/or public interest.

The requirement to provide operational storage and dissemination of high-resolution digital contour maps from recent MDEM data collection activities and the development of new technologies has prompted the need for a major software upgrade and updated design to the MGC. The upgrade, now in the final stages of development, will reflect a new information delivery interface utilizing up-to-date software releases that will lay the groundwork for future upgrades as needed. The design will provide the user with simple and easy routes to the three delivery mechanisms: visualization, information search, and data download. The visualization will utilize the web-browser add-on, Adobe Flex. This easy to navigate and responsive viewer will access ESRI map services and ITS-hosted map and image services. The viewer will retain or improve on available user tools to allow for locating, drawing graphics, measuring, printing, and exporting maps as seen by the user. The information search mechanism will be made more user-friendly by differentiating between MDEM and non-MDEM datasets allowing for a natural flow to data download. GIS data will be available in “Quick Download” packages or through custom online requests.

Mississippi Broadband Report

By Vicki Helfrich
Department of Information Technology Services

On February 9, 2011, the Federal Communications Commission (FCC) released its Notice of Proposed Rulemaking (NPRM) which proposes to reform intercarrier compensation and universal service policies in an attempt to streamline and modernize the current systems. The NPRM proposes four principles to help guide the FCC with comprehensive universal service fund (USF) and intercarrier compensation reform: (1) modernization of the USF and intercarrier compensation systems to make affordable broadband available to all consumers and encourage transformation of circuit-based networks to all IP networks; (2) promotion of fiscal responsibility to control the size of USF as it transitions to support broadband; (3) accountability from companies that receive support

Mississippi Broadband Report

Continued from page six

to ensure public investments deliver intended results; and (4) market-driven and incentive-based policies that encourage deployment of technologies and services that maximize resources and benefit consumers. Specific proposals in the NPRM include:

Eliminate waste and inefficiency throughout the current program.

- Transition funding for duplicative phone service by multiple phone companies operating in the same area to provide support where it's most needed.
- Impose reasonable limits and guidelines for reimbursement to providers that have little incentive under our current subsidy system to operate efficiently.
- Review continued need for funding mechanisms that have not been reevaluated in many years.

Use savings to spur investment in high-speed Internet in unserved areas.

- Identify unserved areas using the forthcoming National Telecommunications and Information Administration (NTIA) national broadband map.
- Create the Connect America Fund to quickly and efficiently deliver support to unserved areas.
- Use market-based policies to support providers in a technology-neutral manner, targeting areas where broadband funding will have the biggest impact.
- Ultimately, streamline and consolidate the USF programs that support rural phone networks into the Connect America Fund. This will constrain spending and bring fixed and mobile broadband to unserved areas while preserving voice service for all, creating jobs and fueling economic growth.

Stimulate investment in broadband by reforming the intercarrier compensation system.

- Eliminate wasteful billing disputes by closing loopholes and tightening rules to prevent "phantom traffic," which is traffic that has been disguised so it can't be identified for billing purposes.
- Amend rules to reduce "traffic pumping," a practice that drains revenues from the system by exploiting existing rules to earn more intercarrier compensation. Reclaimed revenues could be invested in networks or used to reduce prices for consumers.
- Gradually reduce per-minute intercarrier compensation charges. These charges create incentives for carriers to maintain legacy networks that maximize intercarrier revenues rather than investing in advanced, efficient IP-based infrastructure.
- Develop a system to offset reductions in intercarrier rates, including, where necessary, support from the Connect America Fund.

Increase accountability for recipients and for government, and more effectively measure program performance.

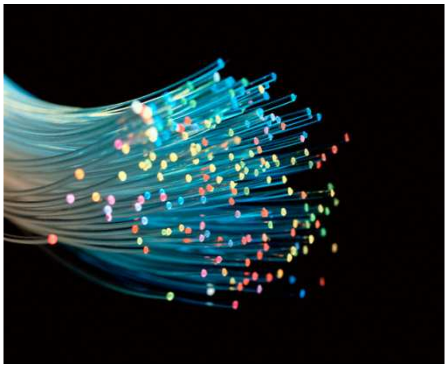
- Adopt clear performance goals and metrics for the Connect America Fund.
- Require increased disclosures about the operating performance and financial condition of companies that receive universal service support.
- Increase transparency, oversight, and accountability.

Mississippi Broadband Report

Continued from page seven

Today, the USF is comprised of four programs:

- High Cost – This support ensures that consumers in all regions of the nation have access to and pay rates for telecommunications services that are reasonably comparable to those in urban areas.
- Low Income – This support, commonly known as Lifeline and Link Up, provides discounts that make basic, local telephone service affordable for more than 7 million low-income consumers.
- Rural Health Care – This support provides reduced rates to rural health care providers for telecommunications and Internet services so they pay no more than their urban counterparts for the same or similar telecommunications services.
- Schools & Libraries – This support, commonly referred to as E-rate support, provides affordable telecommunications and Internet access services to connect schools and libraries to the Internet. This support goes to service providers that provide discounts on eligible services to eligible schools, school districts, libraries, and consortia of these entities.



The NPRM specifically targets the existing high cost program – the component of the USF which supports voice service in high cost, rural and insular areas of the country. The FCC's proposal will re-purpose the high cost mechanism of the USF to support universal broadband availability. Following the goals of the National Broadband Plan, the NPRM proposes to convert the high cost mechanism of the USF to the Connect America Fund through the implementation of several immediate and long-term goals. Tied to this is the intercarrier compensation system which is the fees carriers pay each other to originate, transport, and/or terminate telecommunications traffic. To achieve these goals the FCC proposes to, among other things, eliminate the identical support rule, cap per-line support, implement reverse auctions and redefine funding criteria.

For Your Information

Published by:
Mississippi Department of Information Technology Services
www.its.ms.gov
Contact: Caren Brister
601-432-8198
caren.brister@its.ms.gov